Bell Mobile Device Management (MDM)

Frequently Asked Questions

INTRODUCTION

Bell Mobile Device Management provides business customers an all in one device administration tool to manage multi-platform devices through the entire device lifecycle on a cloud based platform. Bell Mobile Device Management Includes Remote Device Manager which is a Help Desk tool to remotely control, support and troubleshoot mobile devices regardless of user location, this service is exclusive to Bell. Bell Mobile Device Management allows IT Administrators to centrally manage mobile device assets, deliver high quality mobile experience, provide data security, while simultaneously maximizing employee productivity and monitoring the cost of mobile use. The IT Administrator will have insight into applicable mobile devices; have the ability to deploy company policies and simplify technical support via remote access.

TECHNICAL QUESTIONS

What are the prerequisites to operate Bell Mobile Device Management?

Device Management:

- Internet Browser (IE 7, 8, 9; Firefox; Chrome).

Remote Support:

Each agent workstation or Citrix server must have the following software installed:

- Internet Browser (IE 6, 7, 8, 9; Firefox; Chrome).
- Sun Java JRE 1.6 with minimum version of 1.6.17.
- Access ports: Port 80: http; Port 443: SSL-based TCP

The ports must have access to the following IP address:

Server	IP	Port	Region
support.communitake.com	95.211.14.51	80/443	World
support1.communitake.com	46.137.110.154	80/443	World
r1.communitake.com	46.137.110.162	443	Europe
r2.communitake.com	50.19.104.23	443	North America
r3.communitake.com	212.199.177.153	443	Israel
r4.communitake.com	189.1.161.194	443	South America
r5.communitake.com	122.248.248.56	443	Asia

How secure is the Bell Mobile Device Management Application?

All communications are encrypted using industry standard HTTPS and SSL. The private data that is stored on the system server is encrypted. There is a clear segregation between different IT Administrators and end users. One IT Administrator cannot see the information from another IT Administrator and one end user cannot control another end user's device.

The SMS (text) message has not reached the target device, what should the IT Administrator do?

This is probably an SMS gateway issue. Repeat the registration process. The end user can also download the device client directly by directing the device's browser to: http://mydevice.communitake.com/d.
(This manual process is not supported for iOS devices). The IT Administrator can also select the device (or devices) which did not receive the SMS and click "resend SMS".

CommuniTake Technologies Ltd .
Yokneam Star Building, High-Tech Park, POB 344, Yokneam, Israel 20692
E contact@communitake.com P 972-4-959-1608 F 972-4-959-1654

The on-device client installation is stuck, what should the end user do?
The end user's device must have a valid SIM card (BlackBerry devices need a BlackBerry enabled SIM) in order to receive SMS messages and push notifications. On-device client installation may take a few minutes in rare cases. For reinstalling, make sure that the client is not installed on the end user's device. If it is, use the device's "uninstall application" mechanism to make sure that all the files that are related to client are removed. For example, in BlackBerry 9810 devices, long keystroke on the client icon opens a dialog box from-which you can uninstall. The end user would to use the device's remove application program in Options → Device →Application Management.

When the download SMS arrives, make sure that the end user can download and install it normally, as any other application. Once the client has finished installing, the device will show "Successfully Registered" message. If there was no such message, the device did not yet register.

In some cases, the end user may be prompted to enter a PIN code. This PIN code is displayed on the Web application when the device is added to the system. Ensure that there are no network connectivity issues during this process. The client will try to reconnect every few seconds as long as it is running. It will update the capabilities when connected. To make the client simulate a push notification, open the client on the device, click on options and click on "Sync Now".

The IT Administrator does not see a complete view of all the devices in the system dashboard, why?
If the IT Administrator cannot see all the devices, it might indicate that not all the devices have successfully concluded their registration process. The status' can be reviewed via the dashboard view.

None of the Device Management operations are working on the end user's device (backups, location update, application or policy enforcement). Why is it not working?

The speed in which a device will perform a task is directly connected to the speed in which it receives push notifications. Furthermore, a device with no SIM card or an Android device that is not registered, will not receive any push notifications.

The device client handles requests one at a time. If a device has received a command that requires fulfillment time (Get location, for example), and immediately after it, the end user issues a backup request, the backup will not start until the first command finishes and the device connects to the server to get the next command in line. If the client is not properly installed on the device, the device will not publish its actual capabilities to the application server. It means that the application server is not ready to properly issue and manage requests.

Bell Mobile Device Management does not perform "live", "no latency" changes on multiple devices. Requests are published to the device as push notifications via a 3rd party service. Though this usually performs immediately, it might take a few minutes for requests and their driven changes to propagate to the devices.

Can the IT Administrator assign two devices to one end user?
Yes, the IT Administrator would need to simply define another device to the user. The end user doesn't have to be in the same group. Every device will get its policies & configurations based on its group. When the user logs in to the self- service operation, he will see all of his devices.

The IT Administrator would like to swap ownership of a device between end users, can this be done?
The IT Administrator can swap ownership of a device in the same group by clicking "edit" and change the user's name. Moving a device to a different group is not yet supported. The IT Administrator can delete the device and then add it in the required group while attaching it to the new user.

The IT Administrator cannot shift between the Inherit Policy and the Enabled Policy checkboxes.
Make sure to uncheck the Inherit checkbox prior to selecting the Enabled policy checkbox.

How can the IT Administrator know that the inherit policy actually works?
If the parent group has an assigned policy and the inherit checkbox was checked, the inheritance mechanism automatically works. In general, if the OS supports silent install/uninstall then all actions are silent. If not, a notification is displayed to the end user which automatically directs him to the install/uninstall page of the required application. The status can always be seen in the "subscribers" table.

What are the available configurations via the system?
The available configurations include the following: Exchange Activesync; Wi-Fi; VPN; iOS restrictions. A configuration is assigned directly to a group. Inheritance is determined when assigning the group. New groups added after a configuration is created must be manually assigned to the configuration. Configurations are sent only to supporting devices. Some configurations support assigning more than one configuration to a group (for example Wi-Fi).

How can the IT Administrator unlock the device from afar?
If the device is locked and now the IT Administrator wishes to unlock it, remove the assigned password, if there is an assigned one, or indicate it to the device holder.

Can the IT Administrator define application policy via one application for all the devices?
No, as each mobile operating system (OS) has its own built application, even for the same application. For every application that that the IT Administrator wishes to define across multiple mobile OSs, it should specify and include all the relevant OS versions of this application.

What device management features operate on BlackBerry devices?
BlackBerry is designed to be managed via BES. It means that via our system the following occur:

(1) No full remote wipe. The IT Administrator can do selective wipe but it doesn't erase everything, emails for example are not erased
(2) Device lock is done via our on-device client
(3) No password policy

How secured is the lock operation on BlackBerry devices?
As the device lock is done only via our on-device client, the on-device client can be removed by connecting the device to a PC.

When the IT Administrator tries to get the device's location it fails, why?
Getting the device's current location can fail if the device has no GPS reception and is unable to detect its location via the network.

The end user's device does not show the current location.
Click on the refresh tab to generate an accurate device location presentation.

The IT Administrator wants to remove a device from the system, what should they do?
The IT Administrator is to use the remove device mechanism in the devices fleet view. After removing a device, the device should show an alert saying it was disconnected. The device will try to connect to the server and will fail. If no alert is shown, open the client on the device; click on options and then on 'Sync Now'. After the device is successfully disconnected, it can no longer connect to the server. Use the device's application manager to completely uninstall the client, instead of just deleting it.

The IT Administrator cannot delete a group from the groups' hierarchies.
The IT Administrator is to ensure that the group does not contain devices allocated to it. Prior to deletion, a group should be with no devices that are assigned to it.

The IT Administrator has forgotten their login password, what should they do?
The IT Administrator can use the “Forgot my password” link available on the login page to reset the password. If the process was completed successfully you should receive an email with information about how to set a new password.

The IT Administrator has added a device but forgot to add a user for that device, how is that done?
The IT Administrator is to select the “Fleet” tab, click “Edit” and set a user for the device. The new user will receive a welcome email.

The IT Administrator wants to move a device to a different group, how can they do that?
The IT Administrator should delete the device from the system and define it in its new location.

The IT Administrator would like to change the location of a group in the hierarchy. How can they do it?
At present, group change location is not support in the system. In order to move a group location, you will have to delete the devices that are allocated to it, delete the group and define it again in its new location, including devices allocation. Change location will be supported in the near term releases.

The IT Administrator doesn’t always see the same tabs or options when I am managing different devices, why is that?

Two processes occur when an on-device client is properly installed on a device:
1. It publishes the device's management capabilities to the application server. These capabilities vary as different OSs support different capabilities;
2. It automatically changes the system GUI thus allowing for each device to have its own supported features as an operational components in the system GUI. For this reason, not all operations are available in the GUI for some devices.

The IT Administrator is not seeing device diagnostics, why is that?
The device sends a lot of information as part of the registration process. It could be that the device has not yet sent the diagnostics information. The IT Administrator can try and check this page a few minutes later. The diagnostics are updated a few times a day, so they might not represent the exact current information.

The end user does not see the applications on their Android device, why?
The system will present only third party applications that were installed on the device. If the device does not have any such applications, no application will be presented.

The end user cannot do a factory reset on their Blackberry, why?
Blackberry is built to be managed through BES. As such, not all the device management features operate on the Blackberry device. Device manager does not support factory reset on Blackberry devices. The end user can use selective wipe to partly fulfill a factory reset.

Can the end user restore a backup to a different device? How can the end user shift data from one device to another?

These backups are considered as private user information. The restore can be done between different devices in two ways:

(1) If the new device is added with the same phone number as the old device then it will see all the previous device's backups

(2) The user can see backups from all his devices.

Note: Restore can generate duplicated Contacts and Messages. Different devices support different contact attributes. Contacts might be slightly altered and may lose parameters if restored to a different device.

The usage on the expense control is not accurate.

Expense control uses the internal device counters to present the implied usage. These counters are not as accurate as the billing system so some differences may occur. However, the numbers will be accurate enough to monitor the use and generate alerts on exceptional usage.

How can the IT Administrator impose policies?

If an employee does not respond to the device management requests, the IT Administrator can remotely lock the device with their own set password, or block the end user from accessing their email on the device. The device holder will be forced to approach you and fix the policy based on your directive.

How can I know that an employee has uninstalled the on-device application?

You will see that the 'Last seen' indicator will indicate a longer than expected period. In general, the system set to connect to the device every 30 minutes.

What is the process for supporting iOS devices?

You must complete a few simple steps in order to start adding iOS devices to the system:

1. Click "settings" in the top left corner on the Device Manager UI.
2. Fill in the "iPhone certificate request" information and download the certificate request file
3. If you don't already have an Apple ID, please create one (for free) in the following link: http://appleid.apple.com/
4. Sign in using your Apple ID in the following link: https://identity.apple.com/pushcert/
5. Click "create certificate" and agree to the terms of use
6. Upload the certificate request file from step 2, after a few seconds your certificate will be ready for download
7. Upload this certificate in the "Settings" page

How do I add an iOS device to the system?

You start by filling in the device's information, similar to adding any other device.
When opening the link from the SMS/Email, instead of downloading an application, you will download a profile. Accept the installation of the profile to complete the registration process.

What happens when you disable the camera via the iOS restrictions configuration?

When false, the camera is completely disabled and its icon is removed from the Home screen. Users are unable to take photographs.

Can I use the system for managing an iPad or an Android tablet?

Yes. Enter an email address instead of entering a phone number. The download client link will be sent by an email instead of an SMS.

The IT Administrator receives an error when trying to add a new iOS device.

There can be several causes to this error message:

1. The IT Administrator did not register the organization with CommuniTake via Apple. There are a few simple steps that must be done with Apple before the IT Administrator can add an iOS device to the system. Please consult the user manual for more details.
2. The date on the device is incorrect, thus rendering the certificates invalid. Make sure that the device date and year are correct.

The IT Administrator started an import from my LDAP but now cannot open any group.

The import process may take some time depending on the number of groups, users and any changes done in the LDAP from the last time an import was done. During this time, the system blocks access to all the LDAP groups. The status of the import is displayed in the top right corner.

The IT Administrator connected the system with the exchange server and now new devices cannot access their mail.

This means that the exchange settings that were created have blocked all new devices. It means that only devices which are registered to the MDM system can access their mail. Once the IT Administrator adds a new device to the MDM and sets up the exchange account on that device, they must click the device in the “Devices”, go to security and change the device to “allowed” in the exchange configuration.

The IT Administrator would like to allow/block a device from accessing the exchange server but does not see the device in the list.

In order for the system to change the device’s exchange status, the device must first try to connect to the exchange server. Once a connection has been made (even if the device is now blocked) the exchange server “recognizes” the device and the device management system will now be able to find.

The IT Administrator needs to send a status report regarding current system status.

The dashboard can be exported to an Excel file by clicking the “Export” button.

CommuniTake Technologies Ltd .
Yokneam Star Building, High-Tech Park, POB 344, Yokneam, Israel 20692
E contact@communitake.com P 972-4-959-1608 F 972-4-959-1654